J. Symbolic Computation (2002) **34**, 157–172
doi:10.1006/jsco.2002.0554
Available online at http://www.idealibrary.com on IDEAL®

Computing Rational Forms of Integer Matrices

MARK GIESBRECHT† AND ARNE STORJOHANN‡

School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

A new algorithm is presented for finding the Frobenius rational form $F \in \mathbb{Z}^{n\times n}$ of any $A \in \mathbb{Z}^{n\times n}$ which requires an expected number of $O(n^4(\log n + \log \|A\|) + n^3(\log n + \log \|A\|)^2)$ word operations using standard integer and matrix arithmetic (where $\|A\| = \max_{ij} |A_{ij}|$). This substantially improves on the fastest previously known algorithms. The algorithm is probabilistic of the Las Vegas type: it assumes a source of random bits but always produces the correct answer. Las Vegas algorithms are also presented for computing a transformation matrix to the Frobenius form, and for computing the rational Jordan form of an integer matrix.

1. Introduction

In this paper we present new algorithms for exactly computing the Frobenius and rational Jordan normal forms of an integer matrix which are substantially faster than those previously known. We show that the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of any $A \in \mathbb{Z}^{n\times n}$ can be computed with an expected number of $O(n^4(\log n+\log \|A\|)+n^3(\log n+\log \|A\|)^2)$ word operations using standard integer and matrix arithmetic. Here and throughout this paper, $\|A\| = \max_{ij} |A_{ij}|$. The algorithms are probabilistic of the Las Vegas type: they assume the existence of a source of random bits and always return a correct answer. An algorithm is also given which finds a transformation matrix $U \in \mathbb{Q}^{n\times n}$ such that $F = U^{-1}AU$ using an expected number of $O(n^5(\log n + \log \|A\|) + n^4(\log n + \log \|A\|)^2)$ word operations.

Our algorithm for computing F employs a homomorphic imaging scheme: we determine the solution modulo a set of small, randomly selected, primes and recover the integral solution using the Chinese remainder algorithm. We prove that surprisingly few primes are required to ensure correctness of the recovered matrix. Our algorithm for recovering a transformation matrix is fraction-free and returns a $U \in \mathbb{Z}^{n\times n}$. This algorithm is simple to state and requires only integer matrix–vector products plus the computation of the adjoint of an integer matrix.

Intuitively by a *word* we mean a machine word, though we require a formal condition as follows: we assume that a word has at least $\mu = 6 + \left\lceil \log\log(n^{3n^2}\|A\|^{n^2}) \right\rceil$ bits. Motivation for this definition will be derived later, though we note here that $\mu = \Theta(\log n + \log\log \|A\|)$. Practically, $\mu < 48$ on a $10^6 \times 10^6$ matrix where each entry has 10^6 bits, so μ is effectively constant for all reasonable purposes. This definition only affects our complexity estimates, and we may remove this assumption by multiplying

†E-mail: mwg@scg.uwaterloo.ca
‡E-mail: astorjoh@scg.uwaterloo.ca

0747–7171/02/030157 + 16 $35.00/0

costs in word operations by the poly-logarithmic factor μ^2 to obtain costs in bit operations (actually, with some care, a multiple of simply μ suffices).

1.1. MATHEMATICAL BACKGROUND

A classical theorem of linear algebra states that any $n \times n$ matrix A over any field K is similar to a unique block diagonal matrix

$$F = \operatorname{diag}(C_{f_1}, \ldots, C_{f_n}) = \begin{pmatrix} \boxed{C_{f_1}} & & & 0 \\ & \boxed{C_{f_2}} & & \\ & & \ddots & \\ 0 & & & \boxed{C_{f_n}} \end{pmatrix} \in \mathsf{K}^{n \times n}, \tag{1}$$

where each C_{f_i} is the companion matrix of some monic $f_i \in \mathsf{K}[x]$ for $1 \le i \le n$, and $f_i \mid f_{i+1}$ for $1 \le i < n$. We assume for convenience that some of the companion blocks may be empty, or equivalently that there exists a k such that $\deg f_k \neq 0$ and $\deg f_i = 0$ for $k < i \le n$. There exists an invertible *transformation matrix* $U \in \mathsf{K}^{n \times n}$ such that $F = U^{-1}AU$. Recall that the companion matrix C_g of a monic $g = \sum_{0 \le j \le r} b_i x^i \in \mathsf{K}[x]$ has the form

$$C_g = \begin{pmatrix} 0 & & & -b_0 \\ 1 & \ddots & 0 & -b_1 \\ & \ddots & 0 & \vdots \\ 0 & & 1 & -b_{r-1} \end{pmatrix} \in \mathsf{K}^{r \times r}.$$

When g has degree zero (in which case $g = 1$) then C_g is the null matrix with zero rows and columns. A matrix F with the above properties, called the *Frobenius form* of A, always exists and is unique. The polynomials $f_1, \ldots, f_n \in \mathsf{K}[x]$ are the *invariant factors* of A, and the product $f_1 \cdots f_n$ is A's characteristic polynomial, while f_n is A's minimal polynomial. Two matrices are similar if and only if they have the same Frobenius form. Let Δ_i denote the gcd over $\mathsf{K}[x]$ of all $i \times i$ minors of $xI_n - A \in \mathsf{K}[x]^{n \times n}$. Then $f_i = \Delta_i / \Delta_{i-1}$, $1 \le i \le n$, $\Delta_0 = 1$. We will exploit this relationship between the f_i's and Δ_i's in many of our proofs.

When $A \in \mathbb{Q}^{n \times n}$ has all integer entries, the Frobenius form F of A has all integer entries as well. This suggests a simple homomorphic imaging or modular approach to computing $F \in \mathbb{Z}^{n \times n}$ from $A \in \mathbb{Z}^{n \times n}$. One unavoidable difficulty in computing F exactly is that the size of its entries can be quite large: $O(n(\log n + \log \|A\|))$ bits in general. A bigger problem is that the size of intermediate values encountered in any of the previously known non-modular algorithms, can be very large—$O(n^2(\log n + \log \|A\|))$ bits—as can be the entries of a transformation matrix. The modular techniques proposed here are used to avoid some of these problems.

A major difficulty in our homomorphic imaging scheme lies in the fact that some primes are *bad* in the sense that the Frobenius form of A mod p is not equal to F reduced modulo p. The Frobenius form of A mod p might have an entirely different block structure. Examples of this occur when $p \mid \det(A)$ when A is non-singular, or more subtly,

when p divides the discriminant of the minimal polynomial of A. In particular, it is possible that a particular prime may divide the determinant of *all* transformation matrices from A to F. *A priori*, we would seem to require that the product of the chosen primes have $\Omega(n^2(\log n + \log \|A\|))$ bits to ensure that at least one good prime is chosen—this is the best known bound on the number of bits in the determinant of some transformation matrix. We are able to show that in fact we need only compute the Frobenius form modulo a set of primes whose product has $O(n(\log n + \log \|A\|))$ bits.

The Frobenius form is intimately related to the more common Jordan form of a matrix. It is well known that every matrix $A \in \mathsf{K}^{n\times n}$ over an algebraically closed field K is similar to it's Jordan form, a block diagonal matrix $J = \mathrm{diag}(J_1, \ldots, J_\ell)$, unique up to the order of the blocks, where J_i $(1 \leq i \leq \ell)$ is a Jordan block having an eigenvalue of A on the diagonal and ones on the super-diagonal. Such a J does not exist when K does not contain the eigenvalues of A. A natural generalization which always exists is a *rational Jordan form*, a block-diagonal form with companion matrices along the diagonal. The polynomials whose companions form the diagonal are factors of the characteristic polynomials of A. A natural rational Jordan form is obtained by computing a factor refinement on the invariant factors of A. The diagonal of the rational Jordan form then consists of companion matrices of these polynomials (see Kaltofen *et al.*, 1990). This is the most refined rational form one can hope for without factorization in $\mathsf{K}[x]$. The cost to find it is about the same as that of finding the Frobenius form. If the characteristic polynomial is completely factored then a more refined rational Jordan form can be obtained, with the minimal polynomials of the eigenvalues on the diagonal. This factorization is substantially more expensive to compute than the normal form computation itself. Methods to compute transformation matrices to the rational Jordan forms are also exhibited.

1.2. previous work on computing rational forms

Deterministic sequential algorithms for computing the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of an integer matrix $A \in \mathbb{Z}^{n\times n}$ have been proposed by Kannan (1985), Ozello (1987), Lüneburg (1987) and Mathieu and Ford (1990). The p-adic lifting algorithm of Mathieu and Ford (1990) requires about $O(n^6 \log \|A\|)$ bit operations (ignoring logarithmic factors in the input size) using fast integer arithmetic (under an unproven but experimentally justified assumption, which is most certainly true with high probability). Their algorithm does not compute a transformation matrix U to F within this time. Ozello (1987) proposes an algorithm which makes extensive use of large integers for computing the Frobenius form F of an integer matrix A and a transformation matrix to F, which requires about $O(n^8 \log^2 \|A\|)$ bit operations. Ozello also proposes a modular algorithm to compute the Frobenius form but no transformation matrix. While this algorithm is not analyzed, it appears to require about $O(n^5 \log^2 \|A\|)$ bit operations using standard arithmetic. However, Ozello does not address the question of choosing *good* primes p modulo which the Frobenius form of $A \bmod p$ equals $F \bmod p$, and the algorithm stated there may produce incorrect results. Kaltofen *et al.* (1987, 1990) demonstrate fast parallel algorithms for computing the Frobenius and rational Jordan forms of matrices over abstract fields, finite fields and the rationals. While these algorithms are not particularly fast sequentially, we employ some of the techniques developed here in our fast sequential algorithms.

The fastest previously published algorithm for computing exactly the Jordan canonical form of $A \in \mathbb{Z}^{n\times n}$ is by Gil (1992, 1993) and requires about $O(n^9 \log^2 \|A\|)$ bit operations. It appears that a sequential implementation of Kaltofen *et al.*'s (1990) parallel algorithm

for the rational Jordan form requires an expected number of about $O(n^7 \log^2 \|A\|)$ bit operations.

Considerable attention has been paid in the numerical literature to approximating the Jordan form with floating point arithmetic; see Golub and Van Loan (1989), though the numerical sensitivity of the problem has led to concentration on less sensitive (but geometrically less informative) rational forms, such as the real Schur form.

2. Computing the Frobenius Form of a Rational Matrix

Let $A \in \mathbb{Z}^{n\times n}$ have Frobenius form $F = \operatorname{diag}(C_{f_1}, \ldots, C_{f_n}) \in \mathbb{Z}^{n\times n}$. Our modular algorithm computes images $F \bmod p \in \mathbb{Z}_p^{n\times n}$ for sufficiently many primes p to allow recovery of $F \in \mathbb{Z}^{n\times n}$ using Chinese remaindering. Our first task is to bound $\|F\|$. Mathieu and Ford (1990, Section 6), show that if $f \in \mathbb{Z}[x]$ is the characteristic polynomial of A and $h = \sum_{0\le i\le k} c_i x^i \in \mathbb{Z}[x]$ divides f, then

$$\sum_{0\le i\le k} |c_i| \le 2^k \prod_{1\le i\le n} (1 + s_j),$$

where s_j is the 2-norm of the jth column of A, $1 \le j \le n$. Since $s_j \le \|A\|\sqrt{n}$, we have

$$|c_i| \le 2^k(1 + \|A\|\sqrt{n})^n = 2^k\|A\|^n n^{n/2}(1 + 1/(\|A\|\sqrt{n}))^n < 2^k e^{n/2}\|A\|^n n^{n/2},$$

for $1 \le i \le k$, where e is the base of natural logarithms. We get the following:

Lemma 2.1. *Let $A \in \mathbb{Z}^{n\times n}$. Any factor over $\mathbb{Z}[x]$ of A's characteristic polynomial will have coefficients bounded in magnitude by $\gamma = 2^n e^{n/2}\|A\|^n n^{n/2}$.*

Note that this bound is fairly tight, since the best bound we have for the determinant of A in terms of the quantities $\|A\|$ and n is $n^{n/2}\|A\|^n$, Hadamard's bound.

2.1. Identifying and bounding bad primes

For a given prime p, we denote by $F_p = \operatorname{diag}(C_{f_1^{(p)}}, \ldots, C_{f_n^{(p)}})$ the Frobenius form of $A_p = A \bmod p \in \mathbb{Z}_p^{n\times n}$. Let $\Delta_i^{(p)}$ be the GCD over $\mathbb{Z}_p[x]$ of all $i \times i$ minors of $xI_n - A_p \in \mathbb{Z}_p[x]^{n\times n}$, $1 \le i \le n$, $\Delta_0^{(p)} = 1$.

Lemma 2.2. *Let $A \in \mathbb{Z}^{n\times n}$ have Frobenius form F. If p is a bad prime such that the Frobenius form F_p of $A_p = A \bmod p \in \mathbb{Z}_p^{n\times n}$ does not satisfy $F_p = (F \bmod p) \in \mathbb{Z}_p^{n\times n}$, and k is the maximal index for which $f_k^{(p)} \ne f_k \bmod p$, then $\deg f_k^{(p)} < \deg f_k$.*

Proof. The proof is similar to Kaltofen *et al.* (1987, Lemma 4.1). Since Δ_i is monic, we clearly have $\Delta_i \bmod p$ dividing $\Delta_i^{(p)}$, so $\deg \Delta_i^{(p)} \ge \deg \Delta_i$ and $\Delta_i^{(p)} = \Delta_i \bmod p$ in case the degrees are equal. Since $f_i = \Delta_i/\Delta_{i-1}$ we have $\deg f_i = \deg \Delta_i - \deg \Delta_{i-1}$. The maximal $k \in \mathbb{N}$ for which $f_k^{(p)} \ne f_k \bmod p$ is precisely the maximal k with $\Delta_{k-1}^{(p)} \ne \Delta_{k-1}$. But then $\deg f_k^{(p)} = \deg \Delta_k^{(p)} - \deg \Delta_{k-1}^{(p)} = \deg \Delta_k - \deg \Delta_{k-1}^{(p)} > \deg f_k$. □

Now we have the criteria for rejecting bad primes assuming we have one good prime: the reverse degree sequence $(\deg f_n^{(p)}, \ldots, \deg f_1^{(p)})$ of invariant factors of A modulo a

good prime p will be lexicographically greater than the degree sequence of A modulo a bad prime p. Next we bound the product of all distinct bad primes.

LEMMA 2.3. *Let $A \in \mathbb{Z}^{n\times n}$ have Frobenius form F. The product of all bad primes p, for which the Frobenius form F_p of $A_p = A \bmod p \in \mathbb{Z}_p^{n\times n}$ does not satisfy $F_p = F \bmod p \in \mathbb{Z}_p^{n\times n}$, is bounded in magnitude by $n^{3n^2}||A||^{n^2}$.*

PROOF. It follows from Villard (1995) that there exists an $n \times n$ unit lower triangular matrix $C \in \mathbb{Z}^{n\times n}$ with $||C|| \leq n$ and such that the ith diagonal entry of the Hermite normal form $H \in \mathbb{Q}[x]^{n\times n}$ of $(xI_n - A)C \in \mathbb{Z}[x]^{n\times n}$ is equal to the ith invariant factor of A, $1 \leq i \leq n$. Let $H_p \in \mathbb{Z}_p[x]^{n\times n}$ be the Hermite form of $(xI_n - A)C \bmod p \in \mathbb{Z}_p[x]^{n\times n}$. Let d_i and $d_i^{(p)}$ be the degree of the ith diagonal entry of H and H_p, respectively, $1 \leq i \leq n$. A necessary condition for p to be a bad prime is that $(d_1^{(p)}, \ldots, d_n^{(p)}) \neq (d_1, \ldots, d_n)$; in fact the reverse degree sequence $(d_n, \ldots, d_1)$ will be lexicographically greater than $(d_n^{(p)}, \ldots, d_1^{(p)})$ in this case. Note that integer coefficients in $(xI_n - A)C$ will be bounded in magnitude by $\max(\|C\|, \|AC\|) \leq n^2||A||$. Labhalla *et al.* (1996) show that H can be recovered from the reduced row echelon form over $\mathbb{Q}$ of a full row rank matrix $T \in \mathbb{Z}^{n^2\times n(n+1)}$, $\|T\| \leq n^2||A||$. Similarly, H_p can be recovered from the reduced row echelon form over $\mathbb{Z}_p$ of $T_p = T \bmod p \in \mathbb{Z}_p^{n^2\times n(n+1)}$. The degree sequence $(d_1^{(p)}, \ldots, d_n^{(p)})$ will differ from $(d_1, \ldots, d_n)$ only if T_p has a different echelon structure (or rank profile) than T. The rank profile of T is given by $(j_1, \ldots, j_{n^2})$, the lexicographically smallest subsequence of $(1, \ldots, n(n+1))$ such that the $n^2 \times n^2$ minor M comprised of columns $j_1, \ldots, j_{n^2}$ of T is non-zero. A necessary condition for the rank profile of T_p over $\mathbb{Z}_p$ to differ from T over $\mathbb{Z}$ is that $p|M$. The result now follows from Hadamard's bound. □

Lemma 2.3 bounds the length of the product of all bad primes by $O(n^2(\log n + \log ||A||))$ bits. This is asymptotically the currently best known upper bound. It is an open question whether this bound is tight.

2.2. CERTIFYING CORRECTNESS OF THE FROBENIUS FORM

Our next result shows how to assay correctness of a candidate Frobenius form G of A that has been computed using homomorphic imaging with a set of primes having product bounded in length by only $\Theta(n(\log n + \log \|A\|))$ bits.

THEOREM 2.1. *Let $A \in \mathbb{Z}^{n\times n}$ have Frobenius form $F = \mathrm{diag}(C_{f_1}, \ldots, C_{f_n})$. Let $G = \mathrm{diag}(C_{g_1}, \ldots, C_{g_n}) \in \mathbb{Z}^{n\times n}$. If $\|G\| \leq 2^n e^{n/2}\|A\|^n n^{n/2}$, and $G \bmod p$ equals the Frobenius form of $A \bmod p \in \mathbb{Z}_p^{n\times n}$ for a set of primes Λ with $\prod_{p\in\Lambda} > 8^n e^n n^{2n}\|A\|^{3n}$, then $G = F$.*

The proof of Theorem 2.1 depends on a number of intermediate results. We use the fact that any matrix over a field will satisfy precisely those polynomials which are multiples of its minimal polynomial. For any $M \in \mathbb{Z}^{k\times k}$ and any $c \in \mathbb{Z}[x]$ with $\deg c \leq k$, the matrix $c(M)$ will have integer entries bounded by:

$$\|c(M)\| \leq \sum_{0\leq i\leq k} \|c\|k^{i-1}\|M\|^i < 2k^{k-1} \cdot \|c\| \cdot \|M\|^k.$$

Now, if we have an $m \in \mathbb{N}$ with $m > 2k^{k-1} \cdot \|c\| \cdot \|M\|^k$ and $c(M) \bmod m = 0$, then we must have $c(M) = 0$ over $\mathbb{Z}$. We get the following result.

LEMMA 2.4. *Let $M \in \mathbb{Z}^{k\times k}$ and let $c \in \mathbb{Z}[x]$ have degree bounded by k. If $c \bmod p \in \mathbb{Z}_p[x]$ is a multiple over $\mathbb{Z}_p[x]$ of the minimal polynomial of $M \bmod p \in \mathbb{Z}_p^{k\times k}$ for a set of primes Λ with $\prod_{p\in\Lambda} > 2k^{k-1}\cdot\|c\|\cdot\|M\|^k$, then c is a multiple over $\mathbb{Z}[x]$ of the minimal polynomial of M.*

Let g_n be as in Theorem 2.1. From Lemma 2.4 we may deduce that g_n is a multiple of f_n, the minimal polynomial of A. But from Lemma 2.2 we have that $\deg g_n \leq \deg f_n$. We conclude that $g_n = f_n$. Our goal is to extend this certification for g_n to the remaining invariant factors.

It will be useful to define the *order* of one polynomial $h \in \mathsf{K}[x]$ in another polynomial $f \in \mathsf{K}[x]$ as the maximum power of h which divides f. We write $\operatorname{ord}_h f$ for this quantity.

We will need the next two lemmas.

LEMMA 2.5. *Let $T \in \mathsf{K}[x]^{n\times t}$ have rank t, $t < n$. Corresponding to any irreducible $h \in \mathsf{K}[x]$, there exists a*

$$U = \left[\begin{array}{c|c} I_{t+1} & U_1 \\ \hline 0 & I_{n-t-1} \end{array}\right] \in \{0,1\}^{n\times n} \tag{2}$$

with at most one non-zero off-diagonal entry per row, and such that the first $t+1$ rows of UT contain a $t \times t$ minor whose order with respect to h, among all $t \times t$ minors of T, is minimal.

PROOF. Let the minimal order of h amongst all $t \times t$ minors of T be s. Let $(i_1, \ldots, i_t)$ be the lexicographically smallest subsequence of $(1, \ldots, n)$ such that the $t \times t$ minor comprised of rows $i_1, \ldots, i_t$ of T has order s with respect to h. If $i_t \leq t+1$ then $U = I_n$ will satisfy the requirements of the lemma. Assume henceforth that $i_t > t+1$ and choose l minimal with $i_l > t+1$. Let $Q = \operatorname{diag}(Q_1, I_{n-t-1})$ where Q_1 is a $(t+1) \times (t+1)$ permutation matrix such that row j of QT is equal to row i_j of T for $1 \leq j \leq l-1$. Then $(1, \ldots, l-1, i_l, \ldots, i_t)$ is the lexicographically smallest sequence with the $t \times t$ minor comprised of these rows of QT having order, with respect to h, equal to s. Define C to be the $n \times n$ zero matrix except for a 1 in row i column i_j, $l \leq i \leq t$. Then

$$I_n + C = \left[\begin{array}{c|c} I_t & C_1 \\ \hline 0 & I_{n-t} \end{array}\right] \in \{0,1\}^{n\times n}$$

where C_1 has first column zero, first $l-1$ rows zero, and exactly one non-zero entry in the remaining rows. Let $P = \left[\begin{array}{c|c} I_t & C_1 \end{array}\right]$. We claim that $\operatorname{ord}_h(\det(PQT)) = s$. Let Λ be the set of all subsequences of $(1, \ldots, n)$ of length t. For $I \in \Lambda$ let P_I denote the $t \times t$ minor of P comprised of columns I. Similarly, let $(QT)_I$ denote the $t \times t$ minor of QT comprised of rows I. Applying the Cauchy–Binet formula gives $\det PQT = \sum_{I\in\Lambda} P_I\,(QT)_I$ (see Gantmacher, 1990, Section 1.2.4). Since each column of P contains at most a single non-zero entry from $\{0,1\}$, we have $P_I \in \{0,1,-1\}$ for all $I \in \Lambda$. Because s is minimal, we have $(QT)_I \bmod h^{s+1}$ non-zero only if $\operatorname{ord}_h((QT)_I) = s$. To show that $\operatorname{ord}_h \det PQT = s$, it will suffice to demonstrate that there exists precisely one $I \in \Lambda$ for which $P_I(QT)_I$ has

order s with respect to h; in this case the sum $\sum_{I\in\Lambda} P_I(QT)_I \bmod h^{s+1}$ collapses to a single non-zero term. By construction, the submatrix of P comprised of the last $n-(l-1)$ columns has rank $t-(l-1)$. Moreover, amongst the last $n-(l-1)$ columns of P, only columns $l,\ldots,t,i_l,\ldots,i_t$ have a non-zero entry, and these entries lie in rows $l,\ldots,t$. It follows that P_I is non-zero only when $I=(1,\ldots,l-1,j_l,\ldots,j_t)$ with $(j_l,\ldots,j_t)$ a subsequence of $(l,\ldots,t,i_l,\ldots,i_t)$. The lexicographically largest sequence of this form is $I=(1,\ldots,l-1,i_1,\ldots,i_t)$. On the other hand, we have already seen that this is the lexicographically smallest (and hence only) sequence of this form with $\operatorname{ord}_h((QT)_I)=s$. This shows $\operatorname{ord}_h(\det PQT)=s$. It is now easily verified that $U=Q^{-1}(I_n+C)Q$ satisfies the requirements of the lemma. □

Lemma 2.6. *Let $A\in\mathbb{Z}^{n\times n}$. Corresponding to any k $(1\le k\le n)$, and any irreducible $h\in\mathbb{Z}[x]$, there exists a $B\in\mathbb{Z}^{n\times n}$ which satisfies the following:*

- *B is similar to A. Moreover, for any prime p, the Frobenius form of $B \bmod p\in\mathbb{Z}_p^{n\times n}$ equals the Frobenius form of $A \bmod p\in\mathbb{Z}_p^{n\times n}$;*
- *Let M be the principal $k\times k$ submatrix of B. The minimal order of h amongst all $(k-1)\times(k-1)$ minors of xI_k-M is equal to the minimal order of h amongst all $(k-1)\times(k-1)$ minors of xI_n-B;*
- *Entries in M are bounded by $2\|A\|$.*

Proof. Let $t=k-1$. Choose P to be a permutation matrix such that the first t columns of $(xI_n-A)P\in\mathbb{Z}[x]^{n\times n}$ have at least one $t\times t$ minor with minimal order of h. Then $P^{-1}(xI_n-A)P$ also has such a minor occurring in the first t columns. Apply Lemma 2.5 with T the submatrix comprised of the first t columns of $P^{-1}(xI_n-A)P\in\mathbb{Q}^{n\times n}$. This gives us a U as in (2) such that the principal $(t+1)\times t$ submatrix of $UP^{-1}(xI_n-A)P$ contains a $t\times t$ minor with minimal order of h. Note that

$$U^{-1}=\left[\begin{array}{c|c} I_{t+1} & -U_1 \\ \hline 0 & I_{n-t-1}\end{array}\right]\in\{0,1,-1\}^{n\times n},$$

so that post-multiplying a matrix by U^{-1} leaves the first $t+1$ columns unchanged. Thus, the principal $k\times k$ minor of $UP^{-1}(xI_n-A)PU^{-1}$, which is equal to $xI_n-UP^{-1}APU^{-1}$, also has minimal order of h. Then $B=UP^{-1}APU^{-1}$ is easily seen to satisfy the requirements of the theorem. □

We will also need the following, the proof of which is obvious.

Lemma 2.7. *Let $a,b\in\mathbb{Z}[x]$. Then $\|ab\|\le(1+\min(\deg a,\deg b))\cdot\|a\|\cdot\|b\|$.*

Proof of Theorem 2.1. We use proof by contradiction. Assume $G\ne F$ and let $g_k\ne f_k$ for k maximal. By Lemma 2.2 we must have $\deg g_k<\deg f_k$ and we may choose an irreducible factor $h\in\mathbb{Z}[x]$ of f_k with $\operatorname{ord}_h(g_k)<\operatorname{ord}_h(f_k)$. To arrive at a contradiction, we will show that $\operatorname{ord}_h(g_k)\ge\operatorname{ord}_h(f_k)$. Let B be the matrix of Lemma 2.6, M the principal $k\times k$ submatrix of B, g the GCD of all $(k-1)\times(k-1)$ minors of xI_k-M, and Δ_i the GCD of all $i\times i$ minors of xI_n-B, $1\le i\le n$. Then $|xI_k-M|/\Delta_k\in\mathbb{Z}[x]$ and $|xI_k-M|/g$ is the minimal polynomial of M. Let $c=g_k\cdot|xI_k-M|/\Delta_k\in\mathbb{Z}[x]$. Now, if

we can show that c is a multiple of the minimal polynomial of M, that is, show that

$$c = g_k \cdot \frac{|xI_k - M|}{\Delta_k} \text{ is a multiple of } \frac{|xI_k - M|}{g}, \tag{3}$$

then we are finished. To see this, note that $\mathrm{ord}_h(g) = \mathrm{ord}_h(\Delta_{k-1})$ by construction (Lemma 2.6). Then (3) implies

$$\begin{aligned}\mathrm{ord}_h(g_k) &\geq \mathrm{ord}_h(\Delta_k) - \mathrm{ord}_h(g)\\ &= \mathrm{ord}_h(\Delta_k) - \mathrm{ord}_h(\Delta_{k-1})\\ &= \mathrm{ord}_h(f_k).\end{aligned}$$

We now prove (3) using Lemma 2.4. Using $k < n$ (Lemma 2.4), $\|M\| \leq 2\|A\|$ (Lemma 2.6), and $\|c\| \leq (1 + \deg g_k) \cdot \|g_k\| \cdot \||xI_k - M|/\Delta_k\| \leq n \cdot 2^n e^{n/2} A^n n^{n/2} \cdot 2^k e^{k/2} (2\|A\|)^k k^{k/2}$ (Lemmas 2.1 and 2.7), we may derive that

$$2k^{k-1} \cdot \|c\| \cdot \|M\|^k \leq 8^n e^n n^{2n} \|A\|^{3n} < \prod_{p \in \Lambda} p.$$

Thus it will suffice to show that $c \bmod p \in \mathbb{Z}_p[x]$ is a multiple of the minimal polynomial of $M_p = M \bmod p \in \mathbb{Z}_p[x]$ for all $p \in \Lambda$. Let $\Delta_i^{(p)}$ be the GCD of all $i \times i$ minors of $xI_n - B_p$, $1 \leq i \leq n$, $B_p = B \bmod p$. Then $|xI_k - M_p|/\Delta_{k-1}^{(p)}$ is a multiple of the minimal polynomial of M_p. Because k was chosen maximal, we have $\Delta_k^{(p)} = \Delta_k \bmod p$ (see the proof of Lemma 2.2). But then $c \bmod p = (\Delta_k^{(p)}/\Delta_{k-1}^{(p)}) \cdot (|xI_k - M_p|/\Delta_k^{(p)}) = |xI_k - M_p|/\Delta_{k-1}^{(p)}$. □

2.3. Computing the Frobenius form

To compute the Frobenius form, we first choose s random primes p (where s and the selection interval are defined below) and compute the Frobenius form $F_p \in \mathbb{Z}_p^{n \times n}$ of $A_p = A \bmod p$ using any algorithm which has running time bounded by $O(n^3)$ operations from $\mathbb{Z}_p$. A practical deterministic algorithm supporting this running time bound is described in Storjohann (1998). The computation is done independently modulo each p. Let p_0 be a chosen prime modulo which the Frobenius form F_{p_0} of $A \bmod p_0$ has the lexicographically largest reverse degree sequence (p_0 will not be unique). We now bound the probability that p_0 is bad. By Lemma 2.3, there exists a $\delta \in \mathbb{N}$ with $\delta \leq n^{3n^2} \|A\|^{n^2}$ with the property that p_0 is bad only if $p_0 \mid \delta$. Now fix $\mu = 6 + \lceil \log\log \delta \rceil = \Theta(\log n + \log\log \|A\|)$. We will do all our computation modulo primes with μ bits. The following fact guarantees there are enough primes between $2^{\mu-1}$ and 2^μ (it follows easily from the bounds on number-theoretic functions of Rosser and Schoenfeld, 1962):

Lemma 2.8. (Giesbrecht, 1993, Theorem 1.8) *Let $x \geq 3$ and $\mu = 6 + \log\log x$. There exist at least $2\lceil \lceil \log_2(2x) \rceil / (\mu - 1) \rceil$ primes p such that $2^{\mu-1} < p < 2^\mu$.*

An application of this lemma reveals that the product of all primes between $2^{\mu-1}$ and 2^μ is greater than δ^2. In particular, the probability of choosing a bad prime between $2^{\mu-1}$ and 2^μ is at most $1/2$. We generally think of μ as being our machine word size, and that calculations with integers of this size require linear—and practically constant—time. If μ is actually larger than the machine size we can ensure this asymptotic cost by pre-computing the multiplication table for length μ words. This table will have size

$O((n \log \|A\|)^2 \mu)$ bits and the cost of building this table will be dominated by other costs in our algorithms.

Setting $s = \log_2(8^n e^{2n} n^{2n} \|A\|^{3n})/(\mu - 1) = \Theta(n(\log n + \log \|A\|))$, the probability of choosing s bad primes is at most $1/2^s$. By Theorem 2.1, we require s good primes between $2^{\mu-1}$ and 2^μ to recover F from its homomorphic images and to assay correctness. Moreover, by Lemma 2.8 there are more than enough good primes between $2^{\mu-1}$ and 2^μ.

We then proceed as follows. Choose a set Λ_0 of s primes randomly between $2^{\mu-1}$ and 2^μ and compute the Frobenius form F_p of $A \bmod p$ for each $p \in \Lambda_0$. Let $\Lambda_1 \subseteq \Lambda_0$ be those $p \in \Lambda_0$ modulo which the invariant factors $(f_n^{(p)}, \ldots, f_1^{(p)})$ of $A \bmod p$ have maximal degree sequence $(d_n, \ldots, d_1) = (\deg f_n^{(p)}, \ldots, \deg f_1^{(p)})$ of those degree sequences of Frobenius forms of $A \bmod p$ for $p \in \Lambda_0$. We now assume that Λ_1 contains only good primes. We let $\Lambda = \Lambda_1$ initially and proceed to supplement it with more good primes until $\#\Lambda = s$: keep selecting random primes $p \notin \Lambda_0$ between $2^{\mu-1}$ and 2^μ and computing the Frobenius form F_p of $A \bmod p$, adding them to Λ if the reverse degree sequence of the invariant factors equals $(d_n, \ldots, d_1)$. If we find a degree sequence lexicographically greater than $(d_n, \ldots, d_1)$ we were unlucky with our original construction of Λ_1 and must start over, but this happens with probability at most $1/2^s$.

First compute F_p for the s primes $p \in \Lambda$. This requires $O(n^4(\log n + \log \|A\|))$ word operations in total. Recover a $G \in \mathbb{Z}^{n \times n}$ from these images using the Chinese remainder algorithm. This requires $O(n^3(\log n + \log \|A\|)^2)$ word operations. If $||G|| \leq 2^n e^{n/2} \|A\|^n n^{n/2}$, then by Theorem 2.1 we may conclude that G is the Frobenius form of A. If this check on $||G||$ fails, we must start over, but, as noted above, the probability of this happening is at most $1/2^s$.

THEOREM 2.2. *Let $A \in \mathbb{Z}^{n \times n}$. The algorithm described above computes the Frobenius form $F \in \mathbb{Z}^{n \times n}$ of A with an expected number of $O(n^4(\log n + \log \|A\|) + n^3(\log n + \log \|A\|)^2)$ word operations using standard integer arithmetic.*

Note that we consider the computation of a set of $2s$ primes between $2^{\mu-1}$ and 2^μ to be pre-computation but note that they can be computed very quickly using standard sieving methods: see Knuth (1981, Section 4.5.4).

3. Computing Transformation Matrices to the Frobenius Form

Assume that we have the Frobenius form $F \in \mathbb{Z}^{n \times n}$ of an $A \in \mathbb{Z}^{n \times n}$. In this section we describe a simple method to recover a $U \in \mathbb{Z}^{n \times n}$ such that $F = U^{-1} A U$. Let $d_i = \deg f_i$ where f_i is the ith invariant factor of A, $1 \leq i \leq n$. Without loss of generality, we assume

$$F = \begin{pmatrix} \boxed{C_{f_k}} & & & 0 \\ & \boxed{C_{f_{k-1}}} & & \\ & & \ddots & \\ 0 & & & \boxed{C_{f_1}} \end{pmatrix} \tag{4}$$

where $k \in \mathbb{N}$ is maximal with $\deg f_k \geq 1$. Note that (4) simply has blocks in reverse order as compared to (1); we can translate between these two ways of writing the Frobenius form via a similarity transform $P^{-1}FP$ where P is a permutation matrix.

3.1. SIMILARITY TRANSFORM OVER A FIELD

We first develop the algorithm for matrices over a field K. Let $A \in \mathsf{K}^{n\times n}$ have Frobenius form F as in (4). Let L be a subset of K of at least n^2 elements. Choose vectors $w_k, w_{k-1}, \ldots, w_1 \in L^{n\times 1}$ uniformly and randomly. Let $\bar{A}$ be the transpose of A and compute

$$\bar{H} = [w_k|\bar{A}w_k|\cdots|\bar{A}^{d_k-1}w_k|\cdots|w_1|\cdots|\bar{A}^{d_1-1}w_1] \tag{5}$$

where $d_k, d_{k-1}, \ldots, d_1$ is the degree sequence of the invariant factors of F. It is relatively easy to show that if a matrix $\bar{H}$ constructed as in (5) is non-singular, then $\bar{H}^{-1}\bar{A}\bar{H}$ will be in *quasi-Frobenius form*, that is,

$$G = \bar{H}^{-1}\bar{A}\bar{H} = \begin{pmatrix} C_{f_k} & B_{k-1} & \cdots & \\ & C_{f_{k-1}} & & B_1 \\ & & \ddots & \\ 0 & & & C_{f_1} \end{pmatrix} \tag{6}$$

where each matrix B_i is zero except for possibly its last column. If $\bar{H}$ is singular then we made an unlucky choice of $w_k, w_{k-1}, \ldots, w_1$. This is essentially a randomized version of Danilevsky's (1937) algorithm for the characteristic polynomial of a matrix—simplified because we know k and the degrees $d_k, d_{k-1}, \ldots, d_1$. Giesbrecht (1995) shows that H will be non-singular with probability at least $1/4$. Assume henceforth that $\bar{H}$ is non-singular and let H be its transpose. Let $\bar{G}$ be the transpose of the matrix in (6). Then $HAH^{-1} = \bar{G}$ where $\bar{G}$ is block lower triangular with ith diagonal block the transpose of $C_{f_{k-i+1}}$. We now construct a $V \in \mathsf{K}^{n\times n}$ with $V^{-1}\bar{G}V = F$. Let e_i be column $d_i + d_{i+1} + \cdots + d_k$ of I_n for $1 \leq i \leq k$ and set

$$V = [e_k|\bar{G}e_k|\cdots|\bar{G}^{d_k-1}e_k|\cdots|e_1|\cdots|\bar{G}^{d_1-1}e_1]. \tag{7}$$

Now, considering the structure of $\bar{G}$ and choices of the e_i's, it is easily verified that V will be block lower triangular with ith diagonal block non-singular of dimension d_{k-i+1}, $1 \leq i \leq k$. Then V is non-singular and V^{-1} will have a similar block lower triangular structure. Then $V^{-1}\bar{G}V$ is also block lower triangular with ith diagonal block of dimension d_{k-i+1}, $1 \leq i \leq k$. On the other hand, from the non-singularity of V we have that $V^{-1}\bar{G}V$ is in quasi-Frobenius form—and hence block upper triangular. We conclude that $V^{-1}\bar{G}V = F$. We offer the following example over $\mathbb{Z}_7$.

$$
\underset{V^{-1}}{\left[\begin{array}{ccccc|cc|c}
2 & 0 & 2 & 6 & 1 & & & \\
0 & 2 & 6 & 1 & & & & \\
2 & 6 & 1 & & & & & \\
6 & 1 & & & & & & \\
1 & & & & & & & \\
\hline
6 & 3 & 6 & 6 & & 1 & 4\ 1\ 1 & \\
3 & 6 & 6 & & & 4 & 1\ 1 & \\
6 & 6 & & & & 1 & 1 & \\
6 & & & & & 1 & & \\
\hline
 & & 6 & 5 & & 3 & 6 & 4\ 1 \\
 & & 5 & & & 6 & & 1
\end{array}\right]}
\underset{\bar{G}}{\left[\begin{array}{ccccc|cc|c}
 & 1 & & & & & & \\
 & & 1 & & & & & \\
 & & & 1 & & & & \\
 & & & & 1 & & & \\
1 & 5 & 0 & 5 & 1 & & & \\
\hline
 & & & & & & 1 & \\
 & & & & & & & 1 \\
\hline
4 & 1 & 4 & 1 & 1 & 3 & 6\ 3\ 6 & \\
\hline
 & & 6 & 1 & 2 & 3 & 4\ 1 & 1 \\
 & & & & & & & 4\ 3
\end{array}\right]}
\underset{V}{\left[\begin{array}{ccccc|cc|c}
 & & & & 1 & & & \\
 & & & 1 & 1 & & & \\
 & & 1 & 1 & 6 & & & \\
 & 1 & 1 & 6 & 4 & & & \\
1 & 1 & 6 & 4 & 4 & & & \\
\hline
 & & & & 1 & & 1 & \\
 & & & 1 & 1 & & 1\ 6 & \\
 & & 1 & 1 & 6 & 1 & 6\ 4 & \\
 & 1 & 1 & 6 & 4 & 1 & 6\ 4\ 6 & \\
\hline
 & & & 2 & 2 & 6 & & 1 & 1 \\
 & 2 & 2 & 6 & 2 & & 1\ 6 & 1\ 3
\end{array}\right]}
=
\underset{F}{\left[\begin{array}{ccccc|cc|c}
 & & & & 1 & & & \\
1 & & & & 5 & & & \\
 & 1 & & & 0 & & & \\
 & & 1 & & 5 & & & \\
 & & & 1 & 1 & & & \\
\hline
 & & & & & & 3 & \\
 & & & & & 1 & 6 & \\
 & & & & & & 1\ 3 & \\
 & & & & & & 1\ 6 & \\
\hline
 & & & & & & & 4 \\
 & & & & & & & 1\ 3
\end{array}\right]}
.
$$

Then $V^{-1}HAH^{-1}V = F$ and we may choose $U = H^{-1}V$. We now give a refined method for computing this particular similarity transform U directly from H^{-1}, avoiding the computation of $\bar{G}$ and V. We must have

$$U = H^{-1}V = [v_k|Av_k|\cdots|A^{d_k-1}v_k|\cdots|v_1|\cdots|A^{d_1-1}v_1] \tag{8}$$

for some $v_1, \ldots, v_k \in \mathsf{K}^{n\times 1}$ since every transform to the Frobenius form can be written as in (8). But then $[v_k|\cdots|v_1] = H^{-1}\,[e_k|\cdots|e_1]$ so v_i is column $d_i + d_{i+1} + \cdots + d_k$ of H^{-1}, $1 \le i \le k$. Finally, we make an observation that will be useful in the sequel. Let $d \in \mathsf{K}$ be non-zero. Then $(1/d)V^{-1}HAH^{-1}V^{-1}d = F$. This shows that we may take for v_i column $d_i + d_{i+1} + \cdots + d_k$ of dH^{-1}, $1 \le i \le k$. In particular, we may choose $d = \det(H)$ so that $dH^{-1} = H^{\mathsf{adj}}$, the adjoint of H. To conclude, we summarize the algorithm as follows.

1. Construct $\bar{H}$ as in (5) where $w_k, w_{k-1}, \ldots, w_1 \in L^{n\times 1}$ are chosen uniformly and randomly, L a subset of K with at least n^2 elements. If $\bar{H}$ is singular then repeat with new choices of the w_i's. Otherwise, let H be the transpose of $\bar{H}$.
2. Compute v_i to be column $d_i + \cdots + d_k$ of H^{adj} for $1 \le i \le k$.
3. Construct U as in (8).

THEOREM 3.1. *Let $A \in \mathsf{K}^{n\times n}$ have Frobenius form F. The algorithm described above computes a transformation matrix $U \in \mathsf{K}^{n\times n}$ such that $U^{-1}AU = F$. Step* 1 *requires repetition with probability less than* $3/4$.

3.2. SIMILARITY TRANSFORM OVER THE RATIONALS

Consider running the three-step algorithm just described when $\mathsf{K} = \mathbb{Q}$ and $A \in \mathbb{Q}^{n\times n}$ has all integer entries. First we bound the cost of step (1). Entries of $\bar{H}$ are easily seen to be integers bounded in magnitude by $n^n\|A\|^n$. It follows that $\bar{H}$ can be recovered in $O(n^4(\log n + \log\|A\|))$ word operations with less than n matrix–vector products using standard integer arithmetic. Now compute $\beta = 2(1 + \lceil s_1 \cdots s_n \rceil)$ where s_i is the 2-norm of the ith column of $\bar{H}$. Then $\log\beta = O(n^2(\log n + \log\|A\|))$. By Hadamard's bound and Cramer's rule we have that $\beta > 2\det H$ and $\beta > 2\|H^{\mathsf{adj}}\|$. In particular, the entries in the v_i's will be integers bounded by $\beta/2$ and U will be a matrix of integers with $\|U\| \le n^{n-1}\|A\|^{n-1}\beta/2$, or equivalently, $\log\|U\| = O(\log\beta)$. Recover the v_i's using a homomorphic imaging and Chinese remaindering. At the same time determine if $\bar{H}$ was singular. This costs $O(n^5(\log n + \log\|A\|))$ word operations plus the cost of applying the Chinese remainder algorithm to reconstruct kn integers in the v_i's which are bounded in magnitude by β. U can be constructed in this same cost.

THEOREM 3.2. *Let $A \in \mathbb{Z}^{n\times n}$ have Frobenius form F. The Las Vegas algorithm discussed above recovers a transformation matrix $U \in \mathbb{Z}^{n\times n}$ such that $U^{-1}AU = F$. The algorithm requires an expected number of $O(n^5(\log n + \log\|A\|))$ word operations plus the cost of reconstructing n^2 integers bounded in length by $O(n^2(\log n + \log\|A\|))$ bits using the Chinese remainder algorithm.*

Note: for integers of length $\log\beta = O(n^2(\log n + \log\|A\|))$ bits it is reasonable to assume that fast integer arithmetic is more efficient. We could assume that each integer can be reconstructed in $O(\log(\beta)(\log\log(\beta))^2 \log\log\log(\beta))$ bit operations, as might be done with modern FFT-based methods (see, for example, Gathen and Gerhard, 1999, Section 10.3 and Bernstein, 1998), instead of $O((\log\beta)^2)$ bit operations using standard arithmetic. This leads to an overall complexity of $O(n^5(\log n + \log\|A\|) + n^4(\log n + \log\|A\|)^2)$ word operations to recover U.

4. Computing the Rational Jordan Form of an Integer Matrix

The rational Jordan form $J \in \mathbb{Z}^{n\times n}$ of a matrix $A \in \mathbb{Z}^{n\times n}$ is a generalization of the usual Jordan form. For any monic polynomial $g \in \mathbb{Z}[x]$ of degree r and any $m > 0$, define the *rational Jordan block* $J_g^{(m)} \in \mathbb{Z}^{mr\times mr}$ as

$$J_g^{(m)} = \begin{pmatrix} \boxed{C_g}\boxed{I_r} & & 0 \\ & \ddots & \ddots \\ & & \boxed{I_r} \\ 0 & & \boxed{C_g} \end{pmatrix} \in \mathbb{Z}^{mr\times mr}, \tag{9}$$

where I_r is the $r \times r$ identity and C_g is the companion matrix of g.

Now suppose that $A \in \mathbb{Z}^{n\times n}$ has invariant factors $f_1, \ldots, f_k \in \mathbb{Z}[x]$. Furthermore, assume that we know, or can compute, $g_1, \ldots, g_q \in \mathbb{Z}[x]$ which are squarefree and pairwise relatively prime, and such that we can write

$$f_i = \prod_{0\le j\le q} g_j^{m_{ij}}$$

for $1 \le i \le k$. Following Kaltofen *et al.* (1990), we call $g_1, \ldots, g_q$ a *squarefree relatively prime basis* for $f_1, \ldots, f_k$ (see Bach *et al.*, 1993) and note that A is similar to a matrix

$$J = \operatorname{diag}(J_{g_1}^{(m_{11})}, \ldots, J_{g_1}^{(m_{1k})}, \ldots, J_{g_q}^{(m_{q1})}, \ldots, J_{g_q}^{m_(qk)}) \in \mathbb{Z}^{n\times n}.$$

When $g_1, \ldots, g_q$ are irreducible this canonical form corresponds to the usual Jordan form of A, except that the eigenvalues, which are members of a number field, are replaced by their companion matrices. To compute this complete analogue to the usual Jordan form requires factoring f_k, which is somewhat expensive (it requires $O(n^{6+\epsilon}(\log n + \log\|A\|)^3)$ bit operations for any $\epsilon > 0$ using the algorithm of Schönhage (1984)—this cost will dominate that of the entire rational Jordan form algorithm). A less expensive approach (as suggested by Kaltofen *et al.*, 1990) is to perform factor refinement on $(f_1, \ldots, f_k)$ using the algorithm of Bach *et al.* (1993). This factor refinement is unique, as is the corresponding canonical form of A and requires only $O(n^3(\log n + \log\|A\|)^2)$ word operations to compute from the Frobenius form (and this cost is dominated by the Frobenius form computation).

4.1. COMPUTING A TRANSFORMATION MATRIX TO THE RATIONAL JORDAN FORM

Given the Frobenius form $F \in \mathbb{Z}^{n\times n}$ of $A \in \mathbb{Z}^{n\times n}$ and some factor basis $(g_1, \ldots, g_q)$ for the invariant factors, we can very quickly determine the corresponding rational Jordan form J of A by determining the powers of each g_i in each invariant factor. Constructing a transformation matrix X such that $X^{-1}AX = J$ requires more work and we discuss this now.

We really only need construct a transformation matrix $Y \in \mathbb{Q}^{n\times n}$ such that $Y^{-1}FY = J$ since then $X = UY$ is a transformation matrix from A to J. This is accomplished in two stages. We first construct a transformation matrix $Q \in \mathbb{Z}^{n\times n}$ from F to its *primary rational form* $P \in \mathbb{Z}^{n\times n}$. This is a block-diagonal matrix with companion matrices of powers of the g_i's along the diagonal:

$$P = Q^{-1}FQ = \operatorname{diag}(C_{g_1^{m_{11}}}, \ldots, C_{g_1^{m_{1k}}}, \ldots, C_{g_q^{m_{q1}}}, \ldots, C_{g_q^{m_{qk}}}) \in \mathbb{Z}^{n\times n}.$$

Q's structure is very easy to describe and compute. Since F is in block diagonal form and we can treat each of the blocks independently, we may assume without loss of generality that F has only one invariant factor $f \in \mathbb{Z}[x]$ of degree n and primary form $P = \operatorname{diag}(C_{g_1^{m_1}}, \ldots, C_{g_q^{m_q}})$. If $h_i = f/g_i^{m_i}$ and $r_i = \deg g_i$ for $1 \le i \le q$ we have

$$Q = \Big[\overrightarrow{h_1}|\overrightarrow{xh_1}|\cdots|\overrightarrow{x^{m_1r_1-1}h_1}|\cdots|\overrightarrow{h_q}|\cdots|\overrightarrow{x^{m_qr_q-1}h_q}\Big],$$

where $\overrightarrow{h} = (c_0, c_1, \ldots, c_{n-1})^t \in \mathbb{Q}^{n\times 1}$ for any $h = c_0 + c_1x + \cdots c_{n-1}x^{n-1} \in \mathbb{Q}[x]$. Thus, the coefficients of Q are coefficients of factors of f, and by Lemma 2.1 $\|Q\| \le \gamma = 2^n e^{n/2}\|A\|^n n^{n/2}$.

Once we have computed the primary rational form P of A, we find a transformation matrix $T \in \mathbb{Z}^{n\times n}$ such that $J = T^{-1}PT$. Again, without loss of generality we may assume that $P = C_{g^m}$ where $g = \sum_{0\le i\le r} b_i x^i$ is monic of degree r. Under the standard embedding of $\mathbb{Q}^{rm}$ into $\mathbb{Q}[x]/(g^m)$ our problem is equivalent to finding an ordered basis

$$\mathcal{B} = (h_{1,0}, \ldots, h_{1,r-1}, \ldots, h_{m,0}, \ldots, h_{m,r-1}) \in \big(\mathbb{Q}[x]/(g^m)\big)^{rm}$$

for $\mathbb{Q}[x]/(g^e)$ as a $\mathbb{Q}$-vector space, satisfying the following conditions:

(i) $xh_{1,j-1} \equiv h_{1,j} \bmod g^m$ for $1 \le j < r$,

(ii) $xh_{1,r-1} \equiv -\sum_{0\le j<r} b_j h_{1,j} \bmod g^m$,

(iii) $xh_{i,j-1} \equiv h_{i,j} + h_{i-1,j-1} \bmod g^m$ for $2 \le i \le m$ and $1 \le j < r$,

(iv) $xh_{i,r-1} \equiv h_{i-1,r-1} - \sum_{0\le j<r-1} b_j h_{i,j} \bmod g^m$ for $2 \le i \le m$.

We can rewrite (iii) as

(iii′) $$h_{i,j} \equiv x^j h_{i,0} - \sum_{0\le \ell<j} x^{j-\ell-1} h_{i-1,\ell} \bmod g^m \quad \text{for } 1 \le j < r, \text{ and } 2 \le i \le m,$$

and see that $h_{i,j}$ is uniquely determined by $h_{i,0}$ for $0 \le j < r$ (for any i with $1 \le i \le m$). Multiplying both sides of (iii′) by x at $j = r-1$ we obtain

$$xh_{i,r-1} \equiv x^r h_{i,0} - \sum_{0\le \ell<r-1} x^{r-1-\ell} h_{i-1,\ell} \bmod g^m, \qquad \text{for } 1 \le i \le m,$$

while (iv) can be rewritten as

$$xh_{i,r-1} \equiv h_{i-1,r-1} - \sum_{0\le j<r} b_j \left(x^j h_{i,0} - \sum_{0\le \ell<j} x^{j-\ell-1} h_{i-1,j} \right) \bmod g^m.$$

Equating the right-hand sides of the above two equations we get

$$\begin{aligned} \sum_{0\le i\le r} b_j x^j h_{i,0} = g\cdot h_{i,0} &\equiv \sum_{0\le \ell<r} x^{r-1-\ell} h_{i-1,\ell} + \sum_{0\le j<r} \sum_{0\le \ell<j} b_j x^{j-\ell-1} h_{i-1,j} \\ &\equiv \sum_{0\le j\le r} \sum_{0\le \ell<j} b_j x^{j-\ell-1} h_{i-1,\ell} \bmod g^m \end{aligned}$$

for $2 \le i \le m$. As a solution to this system of modular polynomial equations we then have

$$\begin{aligned} h_{1,0} &= g^{m-1}, \\ h_{1,j} &= x^j g^{m-1}, && \text{for } 1 \le j < r, \\ h_{i,0} &= \left(\sum_{0\le j\le r} \sum_{0\le \ell\le j-1} b_j x^{j-\ell-1} h_{i-1,\ell} \right) \Big/ g && \text{for } 2 \le i \le m, \\ h_{i,j} &= x^j h_{i,0} - \sum_{0\le \ell\le j-1} x^{j-\ell-1} h_{i-1,\ell} && \text{for } 2 \le i \le m \text{ and } 1 \le j < r. \end{aligned}$$

Each of these polynomials h_{ij} has degree less than that of g^m, and hence corresponds directly to the vectors of the basis $\mathcal{B}$. By the derivation this is a solution to our system (i)–(iv) provided that $h_{i,0}$ is a polynomial in $\mathbb{Z}[x]$, i.e. that

$$g \,\Bigg|\, \sum_{0\le j\le r} \sum_{0\le \ell\le j-1} b_j x^{j-\ell-1} h_{i-1,\ell}\ .$$

We show by induction that $g^{m-i} \,|\, h_{i,j}$ for $1 \le i \le m$ and $0 \le j < r$. For $i = 1$ this is obvious for all $0 \le j < r$. Assume it is true for h_{i_0,j_0} with $1 \le i_0 < i$, and $0 \le j < r$. We see $g \cdot h_{i,0}$ is a $\mathbb{Z}[x]$-linear combination of h_{i_0,j_0} with $1 \le i_0 < i$, so g^{m-i+1} divides each term in this summation. Thus $g^{m-i} \,|\, h_{i,0}$. Similarly, $h_{i,j}$ is a $\mathbb{Z}[x]$-linear combination of $h_{i,0}$ and h_{i_0,j_0} for $0 \le i_0 < i$, so $g^{m-i} \,|\, h_j$ for $0 \le j < r$. Therefore, by induction $g^{m-i} \,|\, h_{i,j}$ for $1 \le i \le m$ and $0 \le j < r$, and hence $h_{i,j} \in \mathbb{Z}[x]$.

A transformation matrix T from the companion matrix $C_{g^m} \in \mathbb{Z}^{rm\times rm}$ of g^m to its rational Jordan form, the rational Jordan block $J_g^{(m)}$, is thus

$$T = \left[\overrightarrow{h_{1,0}} | \cdots | \overrightarrow{h_{1,r-1}} | \cdots | \overrightarrow{h_{m,0}} | \cdots | \overrightarrow{h_{m,r-1}} \right] \in \mathbb{Z}^{rm\times rm}.$$

We next examine the sizes of the entries of T, which are all coefficients of the polynomials $h_{i,j}$ for $1 \le i \le m$ and $0 \le j < r$. We prove that $\|h_{i,j}\| \le r^{2m-2}\gamma^m n^{(m-1)/2} 2^{(n+1)(m-1)}$ (where $\gamma = 2^n e^{n/2} \|A\|^n n^{n/2}$ as in Lemma 2.1). Since $h_{1,0} = g^{m-1}$ is a divisor of f (the largest invariant factor of A), each coefficient of $h_{1,j}$ has absolute value at most γ for $0 \le j < r$. For $2 \le i \le m$, $\|g\cdot h_{i,0}\| \le r^2\gamma \cdot \max_{0\le \ell<r} \|h_{i-1,\ell}\|$. Dividing by g and applying Mignotte's (1974) bound on the size of coefficients of factors, it follows that

$$\|h_{i,0}\| \le r^2 \gamma 2^n \sqrt{n} \cdot \max_{0\le \ell<r} \|h_{i-1,\ell}\|.$$

More generally, for $1 \le i \le m$ and $0 \le j < r$,

$$\|h_{i,j}\| \le \|h_{i,0}\| + r \max_{0\le\ell<r} \|h_{i-1,\ell}\| \le r^2\gamma 2^{n+1}\sqrt{n} \cdot \max_{0\le\ell<r} \|h_{i-1,\ell}\|.$$

By a trivial induction we obtain, for $1 \le i \le m$ and $0 \le j < r$, that

$$\|h_{i,j}\| \le (r^2\gamma\sqrt{n}2^{n+1})^{m-1}\gamma \le r^{2m-2}\gamma^m n^{(m-1)/2}2^{(n+1)(m-1)}.$$

To compute the entries of T is now straightforward. We will first determine the cost in terms of operations in $\mathbb{Z}$, without regard for their sizes, since our ultimate goal is a modular algorithm. For $i = 1$ we can compute $h_{i,j} = x^j g^{m-1}$ with $O(r^2m^2)$ operations in $\mathbb{Z}$ (we are given g^m). For $1 < i \le m$, assume we have computed h_{i_0,j_0}, with $1 \le i_0 < i$ and $0 \le j_0 < r$. First, compute $\sum_{0\le\ell<j} x^{j-\ell-1}h_{i-1,\ell}$ for $0 \le \ell < r$. This can be accomplished with $O(r^2m)$ operations in $\mathbb{Z}$. Computing $h_{i,0}$ can then be computed with $O(r^2m^2)$ additional operations in $\mathbb{Z}$. Moreover, using the pre-computed $\sum_{0\le\ell<j} x^{j-\ell-1}h_{i-1,\ell}$ for $0 \le \ell < r$, we can find all of $h_{i,j}$, for $1 \le j < r$, with a total of $O(r^2m^2)$ operations in $\mathbb{Z}$. Thus, we determine all coefficients of all $h_{i,j}$'s, and hence all entries in the transformation matrix T, with $O(r^2m^3)$ operations in $\mathbb{Z}$. We have shown the following:

LEMMA 4.1. *Given a matrix $P \in \mathbb{Z}^{n\times n}$ in primary normal form, with $\|P\| \le \gamma$, there exists a matrix $T \in \mathbb{Z}^{n\times n}$ such that $T^{-1}PT$ is in rational Jordan form, and such that $\|T\| \le n^{(3n-1)/2}2^{n^2-1}\gamma^n$. The matrix T can be computed with $O(n^3)$ operations in $\mathbb{Z}$.*

We now discuss how to actually compute Q and T so that UQT is a transformation matrix to the rational Jordan form. Since the entries of Q and T are *polynomials* in the entries of F, we can determine them uniquely through a homomorphic imaging scheme modulo any collection $\Lambda \subseteq \mathbb{N}$ of primes with product greater than ξ, where ξ is defined by

$$\begin{aligned} 2\|UQT\| &\le 2n^2 \cdot \|U\| \cdot \|Q\| \cdot \|T\| \\ &\le 2n^2 \cdot n^{n-1}\|A\|^{n-1}\beta/2 \cdot \gamma \cdot n^{(3n-1)/2}2^{n^2-1}\gamma^n \\ &\stackrel{\text{def}}{=} \xi. \end{aligned}$$

Assume that we have computed F and U as in Theorem 3.2. Modulo any prime $p \in \Lambda$, we can compute $Q \bmod p$ and $T \bmod p$ as above with $O(n^3)$ operations in $\mathbb{Z}_p$. Thus, the cost of computing $UQT \bmod p$ is dominated by that of multiplying these matrices together, and hence can be done with $O(n^3)$ operations in $\mathbb{Z}_p$. If all the primes $p \in \Lambda$ satisfy $2^{\mu-1} < p < 2^\mu$ then we can compute UQT modulo all these primes with $O(n^5(\log n + \log\|A\|))$ word operations, plus the cost of reconstructing n^2 integers bounded in length by $O(n^2(\log n + \log\|A\|))$ bits.

THEOREM 4.1. *Let $A \in \mathbb{Z}^{n\times n}$. The Las Vegas algorithm discussed above to compute the rational Jordan form $J \in \mathbb{Z}^{n\times n}$ of A and a transformation matrix $X \in \mathbb{Q}^{n\times n}$ such that $J = X^{-1}AX$ requires an expected number of $O(n^5(\log n + \log\|A\|)$ word operations plus the cost of reconstructing n^2 integers bounded in length by $O(n^2(\log n + \log\|A\|))$ bits using the Chinese remainder algorithm.*

Acknowledgements

We would like to thank the Natural Sciences and Engineering Research Council of Canada and the Ontario Research and Development Challenge Fund for their support.

References

Bach, E., Driscoll, J., Shallit, J. (1993). Factor refinement. *J. Algorithms*, **15**, 199–222.

Bernstein, D. (1998). Fast arithmetic and integer multiplication benchmarks. `ftp://koobera.math.uic.edu/www/speed/mult.html`.

Danilevsky, A. (1937). The numerical solution of the secular equation. *Matem. sbornik*, **44**, 169–171. In Russian.

Gantmacher, F. R. (1990). *The Theory of Matrices*, volume I. New York, NY, Chelsea Publishing Co..

Giesbrecht, M. (1993). Nearly optimal algorithms for canonical matrix forms. Ph.D. Thesis, University of Toronto, p. 196.

Giesbrecht, M. (1995). Nearly optimal algorithms for canonical matrix forms. *SIAM J. Comput.*, **24**, 948–969.

Gil, I. (1992). Computation of the Jordan canonical form of a square matrix (using the Axiom programming language). In *Proceedings of ISSAC'92*, pp. 138–145. Berkeley, USA.

Gil, I. (1993). Contribution à l'algebre linéaire formelle. Formes normales de matrices et applications. Ph.D. Thesis, Intitut National Polytechnique de Grenoble, Grenoble, France.

Golub, G., Van Loan, C. (1989). *Matrix Computations*. Baltimore, USA, Johns Hopkins University Press.

Kaltofen, E., Krishnamoorthy, M. S., Saunders, B. D. (1987). Fast parallel computation of Hermite and Smith forms of polynomial matrices. *SIAM J. Algebr. Discrete Methods*, **8**, 683–690.

Kaltofen, E., Krishnamoorthy, M. S., Saunders, B. D. (1990). Parallel algorithms for matrix normal forms. *Linear Algebr. Appl.*, **136**, 189–208.

Kannan, R. (1985). Polynomial-time algorithms for solving systems of linear equations over polynomials. *Theor. Comput. Sci.*, **39**, 69–88.

Knuth, D. E. (1981). *The Art of Computer Programming, Seminumerical Algorithms*, volume 2, 2nd edn. Reading, MA, Addison-Wesley.

Labhalla, S., Lombardi, H., Marlin, R. (1996). Algorithmes de calcul de la réduction de Hermite d'une matrice à coefficientspolynomiaux. *Theor. Comput. Sci.*, **161**, 69–92.

Lüneburg, H. (1987). *On Rational Normal Form of Endomorphisms: A Primer to Constructive Algebra*. Mannheim, Wissenschaftsverlag.

Mathieu, M., Ford, D. (1990). On p-adic computation of the rational form of a matrix. *J. Symb. Comput.*, **10**, 453–464.

Mignotte, M. (1974). An inequality about factors of polynomials. *Math. Comput.*, **28**, 1153–1157.

Ozello, P. (1987). Calcul exact des formes de Jordan et de Frobenius d'une matrice. Ph.D. Thesis, Université Scientifique Technologique et Medicale de Grenoble.

Rosser, J. B., Schoenfeld, L. (1962). Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, **6**, 64–94.

Schönhage, A. (1984). Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm. In *Proceedings of ICALP 84*, volume 172 of *Springer Lecture Notes in Computer Science*, pp. 436–447.

Storjohann, A. (1998). An $O(n^3)$ algorithm for the Frobenius form. In *Proceedings of ISSAC'98*, pp. 101–104. Rostock, Germany.

Villard, G. (1995). Generalized subresultants for computing the smith normal form of polynomial matrices. *J. Symb. Comput.*, **20**, 269–286.

von zur Gathen, J., Gerhard, J. (1999). *Modern Computer Algebra*. Cambridge, UK, Cambridge University Press.

Received 29 March 2000
Accepted 23 May 2002